ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(СПбГУ)

Кафедра вычислительной физики
Направление «Прикладные математика и физика»

КВАНТОВЫЕ ИНФОРМАЦИОННЫЕ АЛГОРИТМЫ С НЕПРЕРЫВНЫМИ ПЕРЕМЕННЫМИ

Бакалаврская работа студентки
Дьяковой Оксаны Евгеньевны

Научный руководитель:
к.ф.-м.н., доц., **Яревский Е.А.**

Рецензент:
Карпов Е.А., к.ф.-м.н., с.н.с. СУБ

Санкт-Петербург

2017

Оглавление

Введение ... 3

Литературный обзор ... 4

1. Основные понятия квантовой теории информации ... 6

Бит и кубит ... 6

Квантовые вычисления и схемы ... 6

Квантовая суперпозиция ... 8

Квантовая запутанность ... 8

Теорема о невозможности копирования квантовых состояний ... 9

Граница Холево ... 10

Дискретные и непрерывные переменные в квантовой теории информации ... 11

2. Некоторые квантовые алгоритмы в дискретных переменных и их аналоги в непрерывных переменных ... 13

Квантовая телепортация ... 13

Квантовое копирование ... 15

Алгоритм поиска Гровера ... 16

Алгоритмы, реализуемые только в дискретных переменных ... 17

3. Машинное обучение в квантовой теории информации ... 19

Алгоритм инверсии матриц ... 19

Поиск собственных значений ... 20

Вычисление векторного расстояния ... 20

4. Практическая реализация квантовых вычислений ... 21

Тезис Чёрча-Тьюринга-Дойча ... 21

Квантовый компьютер ... 23

Quipper как высокоуровневый язык программирования для квантовых вычислений ... 24

Заключение ... 26

Список литературы ... 28

Введение

В современном мире информация представляет собой один из наиболее ценных ресурсов, а информационные технологии стремительно развиваются. Поэтому в теории информации на первый план выходит защита данных при хранении и передаче другим лицам. Эту задачу нельзя отнести к новым задачам теории информации: появилась она не с повсеместным распространением компьютерных технологий, а намного раньше. Задача шифрования информации для безопасного хранения и безопасной передачи данных возникла около 4 тыс. лет назад. В наши дни человечество существенно продвинулось в этой сфере, однако на этом развитие не останавливается – параллельно с совершенствованием защиты данных совершенствуются и методы атак для ее взлома.

Наряду с классической теорией информации все большее значение приобретает квантовая теория информации, основанная на некоторых интересных эффектах квантовой механики. К таким эффектам относится, например, квантовая запутанность, аналогов которой нет в классической механике. Однако в силу сравнительной новизны этой теории ее описание не является полным. На сегодняшний день существует сравнительно небольшое количество квантовых алгоритмов теории информации в дискретных переменных, и не все из них могут быть переведены в непрерывные переменные. Немаловажным преимуществом квантовых алгоритмов перед классическими является их быстродействие: там, где классические алгоритмы работают за полиномиальное время, квантовые способны работать за экспоненциальное время.

В связи с этим *целью данной работы* является изучение основ квантовой теории информации, а также некоторых существующих алгоритмов в дискретных и непрерывных переменных.

Для достижения поставленной цели решались следующие задачи:

- Изучение основ квантовой теории информации, в том числе основных понятий квантовой теории информации;
- изучение существующих квантовых алгоритмов в дискретных переменных и их аналогов в непрерывных переменных;
- знакомство с новейшими исследованиями в области квантовой теории информации;
- изучение основ языка Quipper как способа реализации квантовых вычислений.

Литературный обзор

Квантовая теория информации является развивающейся наукой, не изученной до конца. В связи с этим количество публикаций по этой теме незначительно и в большинстве своем представляют теоретическое описание каких-либо алгоритмов.

Для введения в основы квантовой теории информации была выбрана книга американских специалистов Нильсена М. и Чанга И. «Квантовые вычисления и квантовая информация» [1] (2000г., перевод на русский 2006г.). Книга содержит необходимые сведения из смежных областей для большего понимания материала, а также большое количество разнообразных упражнений. В этом учебнике рассматриваются основные понятия квантовой теории информации, основные квантовые алгоритмы (такие, как квантовая телепортация, алгоритм преобразования Фурье, различные алгоритмы поиска).

Большинство источников по квантовым вычислениям являются описанием различных алгоритмов.

Один из самых красивых и значимых для квантовой криптографии алгоритмов – алгоритм квантовой телепортации [2]. Впервые он был сформулирован для кубитов Беннетом в 1993 году [4]. Пусть Алисе требуется передать Бобу кубит q. Алиса и Боб должны иметь доступ к одному кубиту из связанной пары (a, b). Алиса выполняет измерение пары (q, a) и посылает Бобу классический результат измерений. В свою очередь Боб по полученным данным может конвертировать полученные данные и получить точную копию состояния q, которое было разрушено Алисой. Позднее этот алгоритм был расширен на непрерывные переменные – Браугштейн и Кимбл, 1998 г. [5], Ральф и Лэм, 1998 г. [9] и Вейдман, 1994 г. [10].

Другой важный алгоритм – квантовое копирование – запрещен теоремой о невозможности квантового клонирования [11]. Поэтому под этим термином подразумевается алгоритм создания почти совершенных копий, концепт таких клонирующих машин впервые был предложен Бужеком и Хиллери в 1996г. [12]. В 2000 году Церф и Линдбалд предложили его расширение на случай непрерывных переменных [13, 14].

Алгоритм поиска Гровера [15] был предложен в 1996 г. и заключается в решении задачи перебора с помощью оракула – черного ящика. В непрерывном случае используется гамильтониан квантовой системы или

адиабатическое изменение состояния $|0\rangle$. Один из вариантов непрерывного алгоритма Гровера был предложен в 2000 г. [16].

Актуальное в современном мире машинное обучение также не обходится без квантовых алгоритмов. Группа физиков из Теннеси обобщила некоторые алгоритмы, полезные в машинном обучении, на непрерывные переменные, о чем было недавно сообщено в Physical Review Letters [17]. В своей статье они приводят описание трех основных квантовых алгоритмов в непрерывных переменных: алгоритм инверсии матриц, поиск собственных значений и вычисление векторного расстояния.

Некоторые алгоритмы возможны только в дискретных переменных. К таким, например, относятся алгоритм факторизаций Шора [19], алгоритм вычисления дискретного логарифма Шора [19] и алгоритм Саймона [20]. Однако эти алгоритмы имеют большое значение, в особенности для криптографии.

1. Основные понятия квантовой теории информации

Бит и кубит

В основе классической теории информации лежит понятие бита. Бит представляет собой единицу измерения информации в двоичной системе счисления, название образовано от английского словосочетания binary digit – двоичное число. В качестве физической реализации чаще всего используется триггер, который может находиться только в двух устойчивых состояниях (нулевой и высокий). Иначе бит можно интерпретировать как электрический разряд (0 при его отсутствии и 1 при его наличии).

В основе квантовой теории информации бит заменяется на кубит (quantum bit – квантовый бит) и представляет собой квантовый разряд или наименьший элемент для хранения информации в квантовом компьютере. Как и бит, кубит имеет два собственных состояния – $|0\rangle$ и $|1\rangle$ (в обозначениях Дирака). Основное отличие кубита от бита состоит в том, что кубит может также находиться в суперпозиции этих состояний, т.е. в состоянии $\alpha|0\rangle + \beta|1\rangle$, где α и β – комплексные числа, удовлетворяющие условию $|\alpha|^2 + |\beta|^2 = 1$. Термин qubit был введен С. Визнером в 1983 г [3]. При измерении кубита его состояние разрушается, в результате будет получено либо состояние $|0\rangle$ с вероятностью $|\alpha|^2$, либо состояние $|0\rangle$ с вероятностью $|\beta|^2$, так что геометрически кубит можно интерпретировать как единичный вектор в двумерном комплексном пространстве, а квантовые операторы – как действие унитарных матриц на вектора.

Фейнман, породивший квантовую теорию информации своей речью на конференции «Physics of Computation» в Массачусетском Технологическом институте, предлагал в качестве физической реализации кубита фотоны, а в качестве возможных состояний кубита – вертикальную и горизонтальную поляризацию фотонов. В дальнейшем были предложены другие реализации кубитов, такие, как спины ядер и электронов, квантовые точки, NV-центры в алмазах, захваченные ионы и атомы и другое.

Квантовые вычисления и схемы

Квантовые вычисления – язык для описания изменения квантового состояния. Классический компьютер строится из электрических схем, содержащих провода и логические элементы, что позволяет передавать классическую информацию и управлять ей. Квантовый компьютер удобно представлять аналогично классическому компьютеру в виде квантовых схем

из проводов и квантовых элементов, которые позволяют передавать квантовую информацию и управлять ей.

Для примера рассмотрим один из важнейших для квантовых схем оператор CNOT (controlled-NOT). Это простейший элемент на двух кубитах, один из которых является управляющим, а второй – управляемым. Его условное обозначение представлено на рис. 1, где верхняя линия представляет собой управляющий кубит, а нижняя – управляемый.

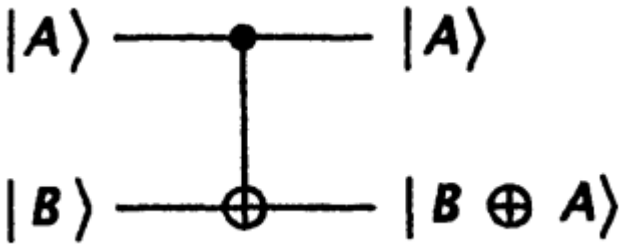

Рис. 1. Условное обозначение элемента CNOT

Если управляющий кубит установлен в 1, то управляемый кубит изменяет свое состояние, если управляющий кубит установлен в 0, то значение управляемого кубита не изменяется. Формальная запись выглядит следующим образом:

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11 \rightarrow |10\rangle.$$

Иначе элемент CNOT можно представить как обобщение классического элемента XOR и описать его действие как $|A, B\rangle \rightarrow |A, A \oplus B\rangle$, где операция $\oplus$ представляет собой сложение по модулю 2 (то, что выполняет логический оператор XOR).

Другой способ описать элемент CNOT – дать его представление в матричной форме для воздействия на вектора вероятности вида $(\alpha_1, \beta_1, \alpha_2, \beta_2)^{\mathrm{T}}$, где α_1, β_1 описывают состояние управляющего кубита, а α_2, β_2 – состояние управляемого кубита. Матричная форма элемента CNOT, которая записана для порядка амплитуд $|00\rangle, |01\rangle, |10\rangle$ и $|11\rangle$:

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

U_{CN} является унитарной матрицей, поэтому требование сохранения вероятности выполняется.

Квантовая суперпозиция

Как было сказано ранее, кубиты обладают способностью находиться в состоянии квантовой суперпозиции, что означает возможность их существования не только в состояниях $|0\rangle$ и $|1\rangle$, но и в промежуточных вида $A|0\rangle + B|1\rangle$, где A и B – комплексные числа, удовлетворяющие условию $|A|^2 + |B|^2 = 1$. Возникает вопрос, как из готовых состояний $|0\rangle$ и $|1\rangle$ можно получить состояния суперпозиции. Одним из возможных способов является элемент Адамара, который переводит состояние $|0\rangle$ в состояние $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, а состояние $|1\rangle$ – в состояние $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Рассмотрим его подробнее.

Элемент Адамара H является унитарным оператором следующего вида:

$$H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Общая схема действия: $H(A|0\rangle + B|1\rangle) = A\frac{|0\rangle+|1\rangle}{\sqrt{2}} + B\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. В результате получается суперпозиция состояний $|0\rangle$ и $|1\rangle$, вероятность получить каждое равняется $\frac{1}{2}$.

Квантовая запутанность

Квантовая запутанность, или зацепленность, важнейшее следствие существования квантовой суперпозиции. Это явление заключается в возникновении взаимозависимости квантовых состояний двух или большего числа объектов. Например, для пары запутанных фотонов существует взаимозависимость спиральности спинов: если при измерении спина одной частицы спиральность оказывается отрицательной, то для второй – всегда положительной, и наоборот. Важную роль в квантовой теории информации играет то, что квантовая запутанность сохраняется даже при разнесении запутанных объектов в пространстве за пределы всех известных взаимодействий. Квантовая запутанность делает возможной существование квантовой коммуникации и квантовой телепортации.

Примером квантовой запутанности являются состояния Белла, или ЭПР-состояния (ЭПР-пары), в честь людей, которые впервые указали на странные свойства подобных пар – Белла и Эйнштейна, Подольского, Розена. Рассмотрим схему их получения (рис. 2).

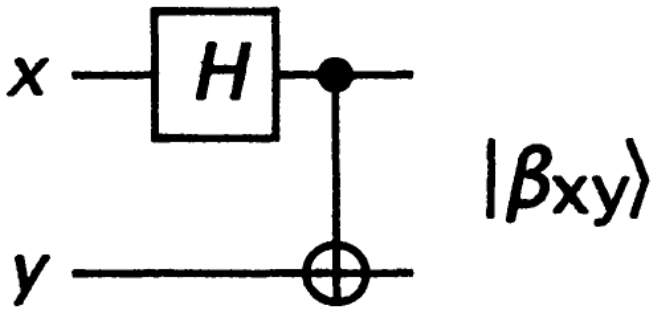

Рис. 2. Квантовая схема получения состояний Белла (ЭПР-состояний)

Возможные входные состояния x и y (а именно, $|0\rangle$ и $|1\rangle$) образуют четыре состояния входного вычислительного базиса: $|00\rangle, |01\rangle, |10\rangle$ и $|11\rangle$. Верхний кубит x приводится в состояние суперпозиции с помощью элемента Адамара, затем эта суперпозиция поступает на управляющий вход элемента CNOT. Управляемый кубит y инвертируется, если значение управляемого кубита равно 1. Выходные состояния, приведенные в табл. 1, и есть запутанные ЭПР-пары. Для примера, если на вход данной квантовой схеме была подана пара $|00\rangle$, то на выходе можно получить только состояния $|00\rangle$ и $|11\rangle$, каждое с вероятностью $\frac{1}{2}$. Состояния $|10\rangle$ и $|01\rangle$ при данном значении входа получить невозможно, что и говорит о возникновении квантовой запутанности между входными кубитами.

Вход	**Выход**
$\|00\rangle$	$\|\beta_{00}\rangle = \frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
$\|01\rangle$	$\|\beta_{01}\rangle = \frac{\|01\rangle + \|10\rangle}{\sqrt{2}}$
$\|10\rangle$	$\|\beta_{10}\rangle = \frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
$\|11\rangle$	$\|\beta_{11}\rangle = \frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

Табл. 1. Квантовая таблица значений входных и выходных состояний схемы получения ЭПР-состояний

Теорема о невозможности копирования квантовых состояний

Классическая информация допускает неограниченное копирование. Однако в квантовой теории информации копирование запрещено соответствующей теоремой [11]. Эта теорема запрещает копирование неортогональных состояний.

Приведем ее доказательство.

Пусть существует некоторое линейное и унитарное преобразование U, которое действует на пару состояний $|a\rangle|0\rangle$ и выполняет следующую эволюцию:

$$U(|a\rangle|0\rangle) = |a\rangle|a\rangle.$$

Поскольку такое «копирующее устройство» должно работать для любых состояний, рассмотрим состояние $|b\rangle \neq |a\rangle$ и применим оператор U к нему:

$$U(|b\rangle|0\rangle) = |b\rangle|b\rangle.$$

Взяв скалярное произведение этих двух уравнений, получаем:

$$\langle a|b\rangle = (\langle a|b\rangle)^2.$$

Отсюда следует, что $\langle a|b\rangle = 0$ или $\langle a|b\rangle = 1$. Первый вариант подразумевает эквивалентность состояний $|a\rangle$ и $|b\rangle$, второй – их ортогональность. Таким образом, создать копирующее устройство для заранее неизвестных состояний, в том числе для тех, процедура получения которых не описана, невозможно.

Граница Холево

Кубиты содержат скрытую информацию, которая теряется при их измерении, однако именно скрытая информация обеспечивает эффективность квантовых вычислений. Граница Холево представляет собой верхнюю оценку доступной информации и играет важную роль во многих применениях квантовой теории информации.

Для определения границы Холево потребуется ввести некоторые важные понятия.

1. Шенноновская энтропия *H(X)* классической случайной величины *X* является мерой количества информации, которое возможно получить, узнав значение *X*. Иначе говоря, это мера неопределенности величины *X* до того, как стало известно ее значение. Пусть величина *X* принимает значения $(x_1,\ldots,x_n)$ с вероятностями $(p_1,\ldots p_n)$. Тогда Шенновскую энтропию можно определить как функцию от распределения вероятностей:

$$H(X) \equiv H(p_1, \dots, p_n) \equiv -\sum_x p_x \log_2 p_x.$$

2. Аналогом энтропии Шеннона в квантовой теории информации служит энтропия фон Неймана квантового состояния ρ, которая определяется как:
$$S(\rho) = \mathrm{tr}(\rho \log_2 \rho).$$
3. Совместная энтропия *H(X, Y)* пары случайных величин является мерой полной неопределенности относительно пары *(X,Y)* и вычисляется следующим образом:
$$H(X,Y) \equiv -\sum_{x,y} p(x,y) \log_2 p(x,y).$$
4. Взаимная информация *H(X:Y)* между *X* и *Y* определяет количество информации, которая является общей для *X* и *Y*. Если сложить информацию *H(X)* и *H(Y)*, то информация, которая содержится только в *X* или только в *Y*, будет учтена один раз, а общая информация – дважды. Поэтому для получения значения взаимной информации необходимо вычесть совместную энтропию:
$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y).$$

Теперь предположим, что Алиса приготавливает состояние ρ_X, где $X = 0, \dots, n$ с вероятностями $(p_1, \dots, p_n)$. Боб проводит измерение над данным состоянием с помощью положительно-определенных операторов $\{E_y\} = \{E_0, \dots E_m\}$, получая результат *Y*. Граница Холево устанавливает, что для любого измерения Боба выполняется неравенство

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x) = \chi,$$

где $\rho = \sum_x p_x \rho_x$.

Величина χ оказалась настолько полезна в квантовой теории информации, что получила название энтропии Холево. Она используется в доказательстве множества результатов квантовой теории информации.

Дискретные и непрерывные переменные в квантовой теории информации

Кубиты являются частным случаем дискретных квантовых переменных и принадлежат конечномерному Гильбертову пространству. Это простейшая квантовомеханическая система в двумерном пространстве с базисными векторами $|0\rangle$ и $|1\rangle$. Операторы в системах с дискретными

переменными имеют дискретный спектр собственных значений. Основным понятием, характеризующим состояние системы, является понятие амплитуды – комплексного коэффициента, который сопоставляется каждому состоянию вычислительного базиса. Если в общем случае кубит находится в состоянии $A|0\rangle + B|1\rangle$, то значения A и B являются амплитудами в соответствующем базисе. Квадрат модуля амплитуды является вероятностью того, что кубит при измерении окажется в соответствующем состоянии. На все вероятности накладывается условие нормировки, которое заключается в том, что сумма всех вероятностей должна равняться единице. В системе из нескольких кубитов ортогональный базис расширяется и является совокупностью всех возможных вариаций состояний отдельных кубитов.

В отличие от систем с дискретными переменными, система с непрерывными квантовыми переменными описывается в Гильбертовом пространстве с бесконечной размерностью. Операторы в системах с непрерывными переменными обладают непрерывным спектром собственных значений, что также отличает такие системы от систем с дискретными переменными.

Два основных шага в квантовых вычислениях на основе непрерывных переменных:

1. Подготовка запутанного состояния кластера, состоящего из квантовых мод как сильно сжатых вакуумных состояний.
2. Проведение одномодовых измерений на соответствующих квантовых модах, где каждый результат используется для выбора последующего базиса измерения.

Примерами квантовых систем с непрерывными переменными могут служить квантованный гармонический осциллятор (непрерывные переменные – координата и импульс, бесконечномерное представление в терминах энергетических состояний), а также бозонные системы квантованных мод, такие, как колебательные моды твердых тел и различные степени свободы электромагнитного поля.

2. Некоторые квантовые алгоритмы в дискретных переменных и их аналоги в непрерывных переменных

Рассмотрим некоторые существующие квантовые алгоритмы в дискретных переменных и их аналоги в непрерывных, если такие существуют.

Квантовая телепортация

Начнем с одного из самых красивых и значимых для квантовой криптографии алгоритмов – квантовой телепортации [2]. Впервые он был сформулирован для кубитов Беннетом в 1993 году [4]. Пусть Алисе требуется передать Бобу кубит q. Алиса и Боб должны иметь доступ к одному кубиту из связанной пары (a, b). Алиса выполняет измерение пары (q, a) и посылает Бобу классический результат измерений. В свою очередь Боб по полученным данным может конвертировать полученные данные и получить точную копию состояния q, которое было разрушено Алисой. Позднее этот алгоритм был расширен на непрерывные переменные – Браугштейн и Кимбл, 1998 г. [5], Ральф и Лэм, 1998 г. [9] и Вейдман, 1994 г. [10].

Квантовая схема механизма телепортации приведена на рис. 3. Две верхние линии принадлежат Алисе, нижняя – Бобу. Телепортируемым состоянием является неизвестное состояние $|\psi\rangle = A|0\rangle + B|1\rangle$. На вход системе подается неизвестное телепортируемое состояние и один кубит из ЭПР-пары, принадлежащий Алисе (второй запутанный кубит находится у Боба). Алиса пропускает свои кубиты через элемент CNOT, а затем первый кубит – через элемент Адамара. Затем Алиса выполняет измерение над парой своих кубитов и посылает классические данные Бобу, который в зависимости от этих результатов может скорректировать данные своих кубитов для получения состояния $|\psi\rangle$.

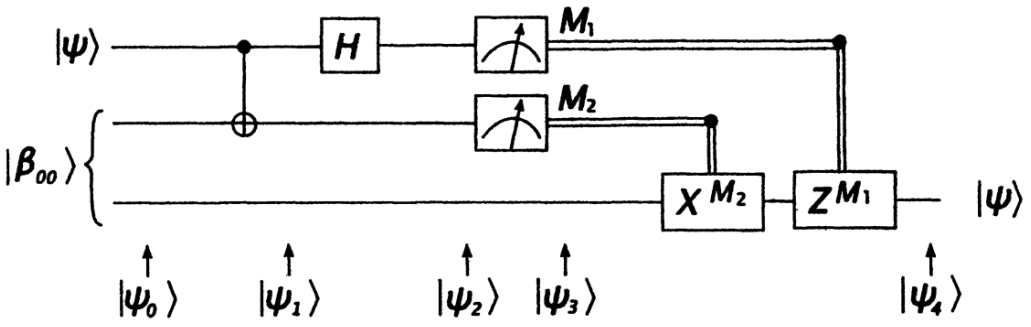

Рис. 3. Квантовая схема телепортации в дискретных переменных

Рассмотрим подробнее изменения состояния кубитов. Состояние на входе системы

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[A|0\rangle(|00\rangle + |11\rangle) + B|1\rangle(|00\rangle + |11\rangle)],$$

где первые два кубита принадлежат Алисе, третий – Бобу. Второй кубит Алисы и кубит Боба находятся в запутанном состоянии. Затем Алиса пропускает свои кубиты через элемент CNOT, получая

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[A|0\rangle(|00\rangle + |11\rangle) + B|1\rangle(|10\rangle + |01\rangle)].$$

Применяя к первому кубиту преобразование Адамара, Алиса получает следующее состояние:

$$|\psi_2\rangle = \frac{1}{2}[A(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + B(|0\rangle - |1\rangle)(|00\rangle + |11\rangle)].$$

Перегруппируем эти слагаемые следующим образом:

$$|\psi_2\rangle = \frac{1}{2}[|00\rangle(A|0\rangle + B|1\rangle) + |01\rangle(A|1\rangle + B|0\rangle) + |10\rangle(A|0\rangle - B|1\rangle) + |11\rangle(A|1\rangle - B|0\rangle)].$$

В результате имеется 4 слагаемых, каждое из которых содержит состояние кубитов Алисы и состояние кубита Боба. Первое слагаемое содержит кубит Алисы в состоянии $|00\rangle$ и кубит Боба в состоянии $A|0\rangle + B|1\rangle$, что соответствует неизвестному состоянию $|\psi\rangle$. Другие возможные состояния кубита Боба приведены в табл. 2. Чтобы Боб мог знать, в каком состоянии находится его кубит, он должен получить результат измерения Алисы, который Алиса передаст по классическому каналу связи.

Результат измерения Алисы	Состояние $\|\psi_3\rangle$ кубита Боба
00	$A\|0\rangle + B\|1\rangle$
01	$A\|1\rangle + B\|0\rangle$
10	$A\|0\rangle - B\|1\rangle$
11	$A\|1\rangle - B\|0\rangle$

Табл. 2. Таблица значений кубита Боба в зависимости от результатов измерения Алисы

В зависимости от результатов измерения Алисы, Боб сможет скорректировать состояние своего кубита с помощью унитарных преобразований X и Z. В случае же, когда результат измерения Алисы 00,

коррекция состояния не требуется – кубит Боба уже находится в искомом состоянии.

Элемент X представлятт собой квантовый элемент NOT, переводя состояние $A|0\rangle + B|1\rangle$ в состояние $A|1\rangle + B|0\rangle$. Элемент Z оставляет $|0\rangle$ без изменений, а $|1\rangle$ переводит в $-|1\rangle$. Ниже приведена их матричная форма и действие на вектор амплитуд состояния кубита.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad X \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} B \\ A \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad Z \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} A \\ -B \end{bmatrix}$$

Как следует из описания алгоритма, на самом деле это не является настоящей телепортацией неизвестного состояния. Состояние, которое было у Алисы, разрушается, чтобы кубит из ЭПР-пары, находящийся у Боба, мог оказаться в нужном состоянии. Тем не менее алгоритм квантовой телепортации играет важную роль для квантовой коммуникации.

Одним из важнейших вариантов алгоритма телепортации в непрерывных переменных является алгоритм *entanglement swapping* (англ. «обмен запутанным») [6,7,8]. Алиса и Боб приготавливают два запутанных двухмодовых состояния, $\hat{\rho}_{aa'}$и $\hat{\rho}_{bb'}$. Моды a и b остаются у Алисы и Боба, a' и b' подвергаются измерениям. На выходе системы получается двухмодовое состояние $\hat{\rho}_{ab}$, где a и b являются связанными.

Квантовое копирование

Другой важный алгоритм - квантовое копирование – запрещен теоремой о невозможности квантового клонирования [11]. Поэтому под этим термином подразумевается алгоритм создания почти совершенных копий, концепт таких клонирующих машин впервые был предложен Бужеком и Хиллери в 1996г. [12]. Такая машина позволяла создать два идентичных клона произвольного кубита. В 2000 году Церф и Линдбалд предложили его расширение на случай непрерывных переменных [13,14]. Их гауссова клонирующая машина создает две копии $(\hat{q}_{1(2)}, \hat{p}_{1(2)})$ входного состояния $(\hat{q}_{in}, \hat{p}_{in})$ с помощью операторов добавления шума, для которых действуют неравенства неопределенности.

Алгоритм поиска Гровера

Алгоритм поиска Гровера [15] был предложен в 1996 г. и заключается в решении задачи перебора с помощью оракула – черного ящика. В непрерывном случае используется гамильтониан квантовой системы или адиабатическое изменение состояния $|0\rangle$. Один из вариантов непрерывного алгоритма Гровера был предложен в 2000 г. [16].

Схема алгоритма Гровера в дискретных переменных приведена на рис. 4. Алгоритм заключается в поиске решения уравнения $f(x) = 1$, где f есть булева функция от n переменных. Классические алгоритмы поиска требуют прямого перебора всех $N = 2^n$ вариантов, в то время как использование квантового параллелизма и вероятностного характера квантовых вычислений сокращает количество перебираемых вариантов до $\frac{\pi}{4}\sqrt{N}$.

Пусть I_a – унитарный оператор, зеркально отражающий гильбертово пространство относительно гиперплоскости, перпендикулярной вектору a, $|x_{tar}\rangle$ — состояние, соответствующее корню уравнения $f(x) = 1$, а состояние $|\tilde{0}\rangle = \frac{1}{\sqrt{N}}\sum_j |j\rangle$ — равномерная суперпозиция всех состояний. Тогда алгоритм поиска Гровера заключается в применении оператора $G = -I_{\tilde{0}} I_{x_{tar}}$ к состоянию число раз, равное целой части $\frac{\pi}{4}\sqrt{N}$. Результат будет близок к состоянию $|x_{tar}\rangle$.

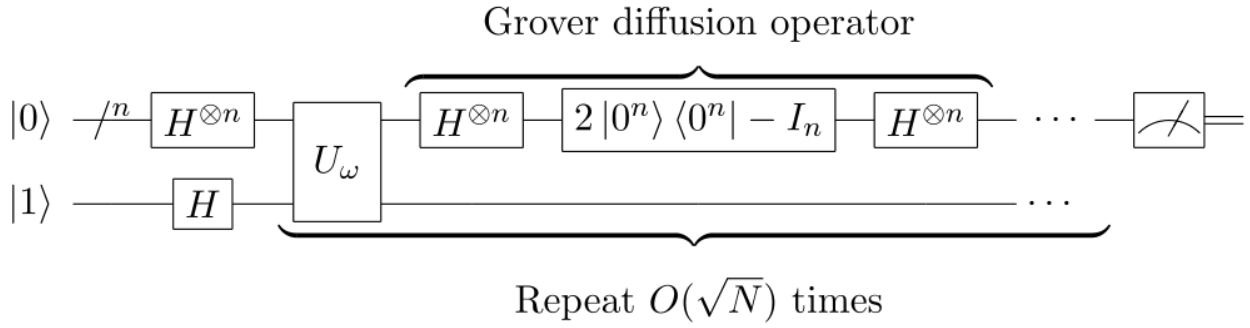

Рис. 4. Квантовая схема дискретного алгоритма Гровера

В системах с непрерывными переменными используется гамильтониан квантовой системы, имеющий вид $H = H_1 + H_2$, где $\exp(iH_1)$ представляет собой оператор $I_{\tilde{0}}$, а $\exp(iH_2)$ – оператор $I_{x_{tar}}$. Эволюция системы с таким гамильтонианом приводит к $|x_{tar}\rangle$ из начального состояния $|\tilde{0}\rangle$, причем сложность данного непрерывного аналога равна сложности дискретного алгоритма Гровера.

Схема Гровера является базовым алгоритмом поиска и используется в нескольких других алгоритмах, таких, как поиск экстремума целочисленной функции или поиск совпадающих строк в базе данных. Это один из алгоритмов, которые невозможно реализовать на машинах с классической архитектурой, поскольку он эффективно использует вероятностный характер квантовых вычислений. Однако можно смоделировать его поведение на классических компьютерах, что, например, было показано Логиновым О.В. и Цыгановым А.В. с использованием среды разработки Maple [18].

Алгоритмы, реализуемые только в дискретных переменных

Некоторые алгоритмы возможны только в дискретных переменных. К таким, например, относятся алгоритм факторизаций Шора [19], алгоритм вычисления дискретного логарифма Шора [19] и алгоритм Саймона [20]. Эти алгоритмы объединяет нахождение поиска периода, и если для алгоритмов Шора поиск периода является вспомогательным инструментом, то в алгоритме Саймона он является целью.

Алгоритм факторизации Шора заключается в разложении некоторого числа n на множители. Такая задача решена и для классических алгоритмов, однако имеет ограничение на размер числа. Квантовый алгоритм факторизации Шора позволяет факторизовать существенно большие числа, что является важным для криптографии (шифры RSA). В основе квантового алгоритма факторизации Шора лежит поиск периода вида $f(a) = x^a (mod\ n)$, т.е. минимального r такого, что $x^r = 1 (mod\ n)$ начинает повторяться. Поиск этого периода осуществляется с помощью квантового дискретного преобразования Фурье, и именно в этом, по всей видимости, кроется причина того, что этот алгоритм не обобщен на системы с непрерывными переменными: для алгоритма является важной конечность базиса преобразования Фурье.

Квантовый алгоритм вычисления дискретного логарифма Шора по той же причине не обобщен на непрерывные переменные, поскольку использует тот же подход – поиск периода элемента некоторой коммутативной группы.

Квантовый алгоритм Саймона заключается в поиске периода y некоторой квантовой функции $F(x)$, если известно, что $F(x) = F(x + y)$, где операция «+» - побитовый XOR. Решение, предложенное Саймоном в 1994 г.,

приведено на рис. 5 и заключается в использовании элементов Адамара к части кубитов до и после применения квантовой функции *F(x)*.

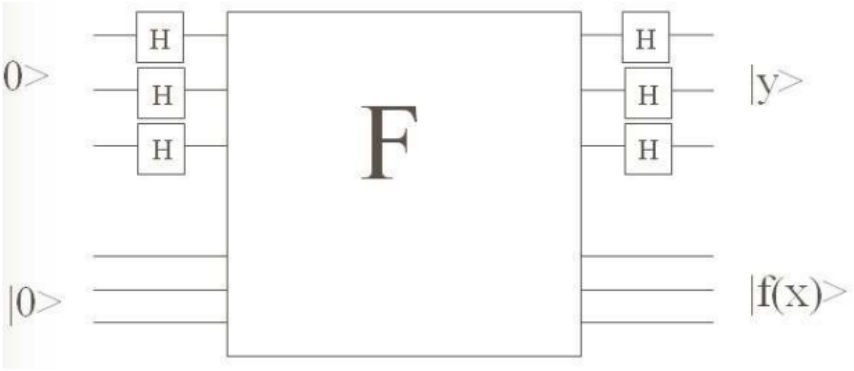

Рис. 5. Квантовая схема алгоритма Саймона

В этом разделе были рассмотрены простейшие, базовые алгоритмы квантовой теории информации. Помимо рассмотренных в этом разделе существуют и более сложные алгоритмы, решающие специфические задачи. Ввиду недолгого существования квантовой теории информации говорить о ее завершенности рано.

3. Машинное обучение в квантовой теории информации

В последнее время набирает популярность сфера машинного обучения, которое является подразделом искусственного интеллекта и включает в себя специально разработанные «алгоритмы обучения». Сфера применения алгоритмов машинного обучения велика, поскольку основная задача – частичная или полная автоматизация решения сложных профессиональных задач, в том числе различное прогнозирование, управление и принятие решений. К таким задачам относятся, например, биржевой анализ, предсказание ухода клиентов, распознавание рукописного текста и звука, медицинская диагностика.

Поскольку эти алгоритмы имеют большую вычислительную сложность, целесообразно использование квантовых алгоритмов, которые могут быть выполнены за экспоненциальное время (в отличие от классических, которые выполняются за полиномиальное время) благодаря эффективному использованию квантового параллелизма.

Квантовые обучаемые алгоритмы относятся к категории машинного обучения. Физики из Теннеси обобщили их часть на непрерывные переменные, о чем было недавно сообщено в Physical Review Letters [17]. Рассмотрим их подробнее.

Алгоритм инверсии матриц

Этот алгоритм имеет особое значение для машинного обучения, поскольку различные приложения машинного обучения включают в себя линейные уравнения больших размерностей, а также их системы $\mathbf{Ay} = \mathbf{b}$. Преимущество квантовых алгоритмов машинного обучения в том, что они способны решать линейные уравнения более эффективно. В частности, в 2009 г. в статье Харроу, Хаззидима и Ллойда [21] было показано, что нахождение вектора решения $\mathbf{y} = \mathbf{A}^{-1}\mathbf{b} = \sum_i {\mathbf{b}_i}/{\lambda_i \mathbf{e}_i}$ для любого вектора $\mathbf{b} = \sum_i \mathbf{b}_i \mathbf{e}_i$ эффективнее вычисляется на квантовом компьютере.

В системе с непрерывными переменными алгоритм начинается с подготовки состояния $|\mathbf{b}\rangle$, а также двух вспомогательных мод в квадратурах q, являющихся квантовомеханическими состояниями, соответствующими собственным значениям волнового уравнения, а именно: $|0\rangle_{\mathrm{q,R}}$ и $|0\rangle_{\mathrm{q,S}}$. Затем оператор $\exp(i\delta\gamma\mathbf{A}\hat{p}_R\hat{p}_S)$ применяется 1/δ раз. После преобразований, получается состояние, в котором пренебрегают константой нормировки.

Если S-вспомогательная мода измерима в q-квадратуре с результатом $\mathrm{q_S}$, то тогда получаем состояние $\sum_i \mathbf{b}_i/\lambda_i|\mathbf{e}_i\rangle\,|q_S/\gamma\lambda_i\rangle_{p,R}$. До нормировки состояние решения $|\mathbf{y}\rangle = \sum_i \mathbf{b}_i/\lambda_i|\mathbf{e}_i\rangle$ достигается при условии, что R-вспомогательная мода измерима в q-квадратуре, и тогда мы получаем, что $\mathrm{q_R}$= 0.

Поиск собственных значений

Другой важной задачей является нахождение собственного значения λ, которое соответствует единичному собственному вектору $\mathbf{e}_i$ относительно матрицы **A**, то есть $\mathbf{A}\mathbf{e}_i = \lambda_i\mathbf{e}_i$. Эта проблема повсеместно распространена в науке и технике.

Алгоритм стартует из состояния данных $|\mathbf{e_i}\rangle$ и вспомогательной моды R, подготовленной как нулевое собственное состояние q-квадратуры, $|0\rangle_{\mathrm{q,R}}$. Идея алгоритма заключается в применении оператора $\mathrm{e}^{i\gamma\mathbf{A}\hat{p}_R}$, который смещает вспомогательную моду в соответствии с её собственным значением, а затем это собственное значение может быть получено путем измерения вспомогательной моды. Этот оператор может быть реализован путем подготовки ансамбля таким образом, чтобы матрица плотности выражалась как $\rho' = \mathbf{A}/\mathrm{tr}\,\mathbf{A}$. На практике, успех алгоритма зависит от различимости состояния $|\gamma\lambda_i\rangle_{\mathrm{q}}$, которая зависит от спектра собственных значений, степени сжатия вспомогательного состояния, а также величины ошибки.

Вычисление векторного расстояния

В контролируемом машинном обучении новые данные классифицируются по группам на основе сходства с предыдущими данными. Например, категория принадлежности вектора **u** определяется расстоянием D до среднего значения предыдущих данных $\{\mathbf{v_i}\}$. Цель алгоритма обучения квантовой машины состоит в вычислении значения $\mathrm{D}^2 \equiv \left|\mathbf{u} - \sum_{\mathrm{i=1}}^{\mathrm{M}} \mathbf{v_i}/\mathrm{M}\right|^2$.

Предполагается, что оракул может генерировать состояние $|\Psi\rangle = \frac{1}{\mathcal{N}}\left(|\mathbf{u}||0\rangle_I|\tilde{\mathbf{u}}\rangle + \frac{1}{\sqrt{M}}\sum_{i=1}^{M}|\mathbf{v}_i||i\rangle_I|\tilde{\mathbf{v}}_i\rangle\right)$, где первая мода обозначается индексом моды I; нормировка $\mathcal{N} \equiv \sqrt{|\mathbf{u}|^2 + \sum_i|\mathbf{v}_i|^2/M}$ предполагается заранее известной. Значение D^2 может быть получено путем проведения теста замены индексов моды с референсной модой, представленной в виде $|\Phi\rangle_R \equiv \left(|0\rangle_R - \sum_{i=1}^{M}|i\rangle_R/\sqrt{M}\right)/\sqrt{2}$.

4. Практическая реализация квантовых вычислений

Тезис Чёрча-Тьюринга-Дойча

Понятие алгоритма является одним из ключевых в теории информации. Первые алгоритмы возникли много веков назад, но точное определение этого понятия было сформулировано только в 30-х годах XX века. В начале прошлого столетия математик Давид Гильберт сформулировал проблему, известную как Entscheidungspronlem: существует ли алгоритм, способный решить все математические задачи. Для того, чтобы ответить на этот вопрос, требовалось формальное определение алгоритма, которое соответствовало бы его интуитивному определению.

В 1936 г. Чёрч и Тьюринг независимо друг от друга сформулировали тезис Чёрча-Тьюринга, который утверждает эквивалентность интуитивного понятия – класса функций, которые вычисляются с помощью алгоритма, и математического понятия – класса функций, которые возможно вычислить на машине Тьюринга. Тезис Чёрча-Тьюринга формулируется так: «класс функций, вычислимых на машине Тьюринга, в точности совпадает с классом функций, вычислимых с помощью алгоритма». Благодаря этому тезису становится возможным изучение строгими математическими методами реальных алгоритмов. Несмотря на то, что на данный момент не найдено опровержение этого тезиса, не исключено существование процесса, вычисляющего функцию, которую нельзя вычислить с помощью машины Тьюринга.

Рассмотрим принципиальное строение машины Тьюринга (см. рис. 6). Она состоит из программы, управляющего устройства с конечным числом состояний, которое работает как простейший процессор и координирует работу машины Тьюринга, ленты, соответствующей памяти компьютера, и читающей/пишущей головки, которая указывает на конкретное место ленты, где в данный момент можно считать данные или записать их.

Среди всех состояний управляющего устройства выделяются начальное состояние, в котором машина Тьюринга находится в начале вычислений, и заключительное состояние, в которое машина Тьюринга приходит после процесса вычислений. Лента является одномерным объектом, простирающимся бесконечно в одну сторону, и представляет последовательность пронумерованных ячеек. В каждой ячейке содержится один символ из некоторого конечного алфавита. Программа машины Тьюринга представляет собой упорядоченный конечный список

программных строк вида (q, x, q’, x’, s), где q – текущее состояние машины, x – символ на ленте, на который указывает головка. Шаг машины Тьюринга заключается в поиске строки, которая соответствует текущему состоянию машины и символу, над которым находится головка. Если такая строка находится, то она исполняется, что заключается в изменении состояния машины на q’, перезаписи символа x на символ x’ и сдвиг головки в соответствием значения параметра s (сдвиг на единицу вправо/влево или отсутствие изменений). С помощью машины Тьюринга можно смоделировать все обычные конструкции языков программирования.

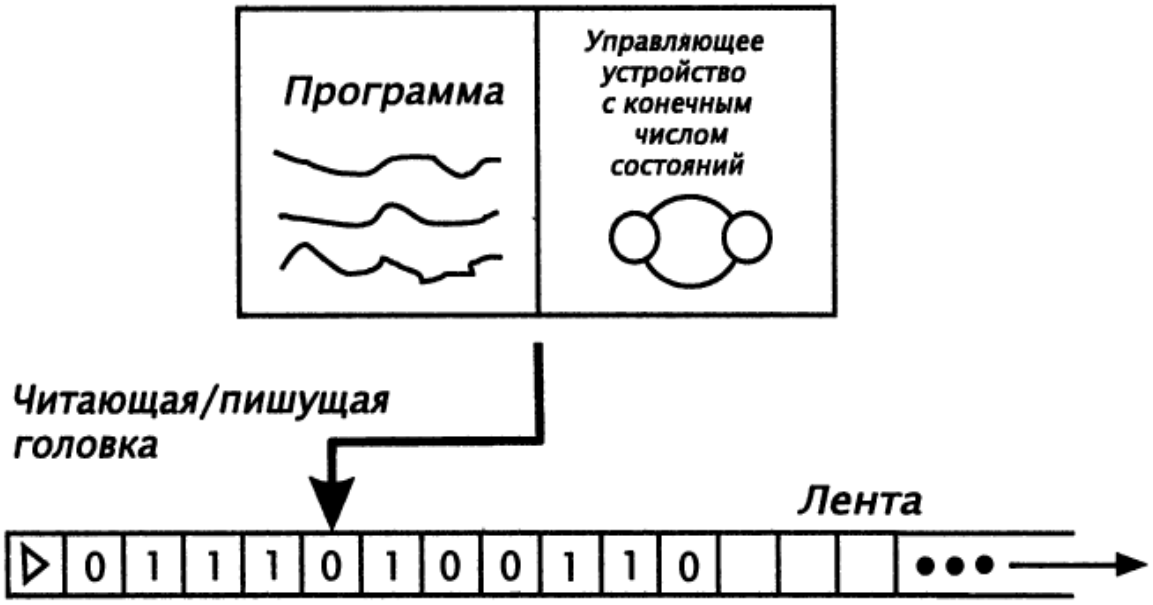

Рис. 6. Принципиальное строение машины Тьюринга

Позднее были сформулированы другие формулировки тезиса Чёрча-Тьюринга. Физический тезис Чёрча-Тьюринга подразумевает, что любая функция, вычислимая с помощью физического устройства, может быть вычислена машиной Тьюринга. В 1985 г. Дойч в своей работе [22] предложил другую формулировку, известную как сильный тезис Чёрча-Тьюринга, тезис Чёрча-Тьюринга-Дойча или CTD-принцип (по аббревиатуре Church, Turing, Deutsch). Согласно этому тезису, универсальное компьютерное устройство способно моделировать любой конечный физический процесс, не использующий аппарат, связанный с непрерывностью и бесконечностью. Однако аппарат классической физики использует понятия непрерывности и континуума, следовательно, он не может моделировать все физические процессы. Дойч предположил существование универсального квантового компьютера, который способен обойти эти ограничения. Для этого

необходимо, чтобы законы квантовой физики являлись теоретической базой для описания любого физического процесса.

Квантовый компьютер

Квантовый компьютер, в отличие от классического компьютера, строится на использовании эффектов квантовой запутанности и квантовой суперпозиции. Поскольку элементарный объект квантовой теории информации в принципе существует в природе, нужно уметь выбрать систему, в которой воплощаются квантовые свойства кубита, управляется их динамика, а также необходимо уметь подготавливать некоторый набор начальных состояний и измерять конечный результат. Как правило, удается удовлетворить лишь части этих требований. Поэтому правильный вопрос не в том, как построить квантовый компьютер, а в том, насколько хороший квантовый компьютер возможно построить. Возможные реализации, такие, как гармонический осциллятор, компьютер на оптических фотонах, ионы в ловушке и некоторые другие, а также их недостатки, подробно описаны в книге Нильсена и Чанга [1] и не приводятся в данной работе.

На данный момент универсальный квантовый компьютер остается гипотетическим устройством, однако уже реализованы единичные экспериментальные системы, выполняющие фиксированный алгоритм небольшой сложности. Одним из таких компьютеров является адиабатический квантовый компьютер D-Wave, права на который в данный момент принадлежат компании Google. Последняя реализация адиабатического компьютера D-Wave – D-Wave 2000q – содержит 2000 кубит (однако не все из них являются попарно запутанными, общий набор распадается на множество регистров до 8 попарно запутанных кубитов (см. рис. 7)).

Этот компьютер работает по принципу квантового отжига, или квантовой нормализации, и представляет собой систему из большого числа компонентов и управляющих параметров. Процесс квантового отжига заключается в поиске глобального минимума посредством заменения текущего решения на соседнее случайным образом, если в соседнем решении оптимизируемый функционал меньше. Этот процесс регулируется параметром «напряженность поля туннелирования», который при старте достаточно велик, поэтому поиск проводится по всему пространству. При уменьшении поля напряженности система «оседает» в нескольких состояниях с минимальными значениями оптимизируемого функционала,

одно из которых будет соответствовать глобальному минимуму. В пределе получается классическая система в одном из основных состояний.

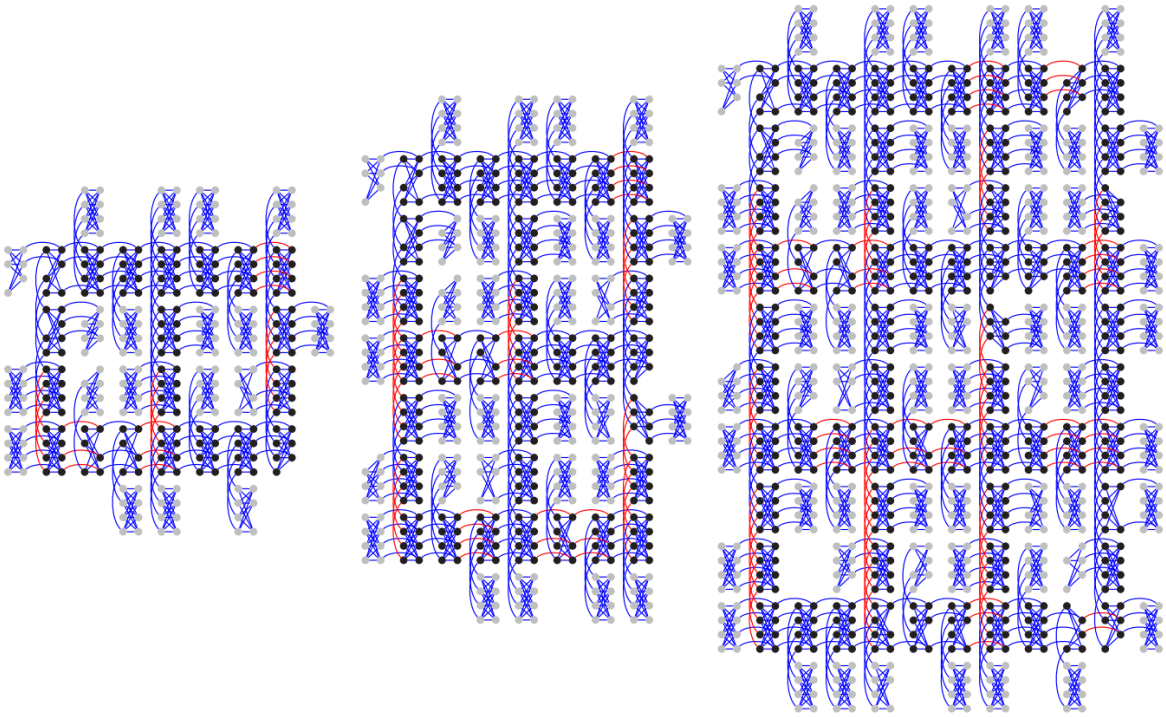

Рис. 7. Общая схема запутанных кубитов компьютеров D-Wave

Квантовый компьютер D-Wave работает при низких температурах и медленно изменяет свое состояние за счет квантового туннелирования при изменении заданных параметров. К сожалению, этот компьютер способен решать ограниченный класс задач оптимизации и не подходит для реализации классических квантовых алгоритмов и квантовых вентилей.

Quipper как высокоуровневый язык программирования для квантовых вычислений

Несмотря на то, что квантовые алгоритмы в непрерывных переменных представляют значительный интерес для исследования, их практическая реализация существующими программными ресурсами не является возможной. Но и для алгоритмов в дискретных переменных есть свои ограничения. Немаловажную роль играет отсутствие полноценных квантовых компьютеров, однако даже на стадии их разработки необходимо понимать,

Язык Quipper [23] относится к языкам программирования высокого уровня и был разработан Петером Зелингером (Peter Selinger) и его командой из университета Дэлхоузи в Галифаксе, Канада, как часть проекта QCS

(Quantum Computer Science) [24] агенства IARPA (Intelligence Advanced Research Projects Activity, агентство передовых исследований в сфере разведки). Проект призван оценить и сократить вычислительные ресурсы, которые требуются для реализации квантовых вычислений на реалистичном квантовом компьютере. Язык Quipper считается первым практическим языком для квантовых компьютеров и был реализован в качестве встроенного языка программирования, основным для него является Haskell, так что Quipper можно рассматривать как совокупность библиотек, типов данных и комбинаторов языка Haskell. При этом Quipper имеет собственную идиому, т.е. предпочтительный стиль написания программы. Дистрибутив для языка Haskell можно свободно установить с официального сайта, посвященного этому языку [25].

Язык Quipper использует расширенную схемную модель квантовых вычислений, в которую включаются квантовые и классические данные и операции над ними. С помощью классических данных можно управлять квантовыми операциями, но не наоборот. Также квантовые данные можно измерить и получить классические.

Использование схемной модели приводит к появлению трех этапов выполнения программы: компиляция, генерация схемы и исполнение схемы, вследствие чего появляются три различных типа данных (битов и кубитов). Входные данные, значение которых известно на стадии генерации схемы, называются параметрами (Bool), а те данные, значения которых известно только на стадии исполнения программы – входными данными (Bit для классических данных и Qubit для квантовых). Вычисления производятся с помощью функций.

К минусам языка Quipper относится незавершенность его разработки. К тому же, как и для всех языков программирования, его использование предполагает только дискретные переменные. Программирование в непрерывных переменных на данном этапе развития науки и техники невозможно.

Заключение

В рамках данной работы было проведено первоначальное погружение в квантовую теорию информации, а также проведено теоретическое исследование нескольких существующих на данный момент алгоритмов квантовой теории информации.

По каждой из поставленных задач можно сделать следующие выводы:

- Были изучены основы квантовой теории информации. Изучены простейшие квантовые схемы и элементы теории кубитов, а также некоторые важные теоремы, такие, как граница Холево, играющая важную роль в квантовой теории информации, и теорема о невозможности копирования квантовых состояний (за исключением ортогональных), которая приведена в данной работе с доказательством.
- Рассмотрены основные алгоритмы квантовой теории информации в дискретных переменных и их обобщения на системы с непрерывными переменными. В качестве объекта рассмотрения были взяты основные алгоритмы, такие, как квантовая телепортация, квантовое копирование и алгоритм поиска Гровера. Некоторые алгоритмы существуют только в дискретных переменных, было дано возможное объяснение невозможности существования этих алгоритмов в непрерывных переменных.
- Новейшие исследования в рамках квантовой теории информации касаются области машинного обучения. Было проведено рассмотрение трех базовых алгоритмов, недавно обобщенных на непрерывные переменные.
- Были изучены потенциальные возможности квантовых компьютеров, а также уже существующих компьютеров D-Wave. Также было проведено знакомство с основами языка Quipper как высокоуровневого языка программирования для квантовых вычислений.

За квантовой теорией информации стоит будущее. Несмотря на то, что классические компьютеры переживают бурный рост развития технологий, ожидается, что в скором времени будет достигнут их предел. К тому же, квантовые компьютеры показывают большую эффективность, чем классические, что делает их интересным объектом для дальнейших исследований.

Дальнейшее исследование квантовой теории информации представляет собой перспективную задачу ввиду неполноты данной теории и ее интенсивного развития.

Список литературы

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ – М: Мир, 2006 г. – 824 с., ил
2. Молотков, Назин «О телепортации непрерывной переменной»
3. S. Wiesner, “Conjugate Coding”, SIGACT News, Vol. 15, No. 1, 1983, pp. 78-88.
4. Bennett, C. H., G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, Phys. Rev. Lett. 70, 1895.
5. Braunstein, S. L., and H. J. Kimble, 1998, Phys. Rev. Lett. 80, 869.
6. Van Loock, P., and S. L. Braunstein, 1999, Phys. Rev. A 61, 010302(R).
7. Jia, X., X. Su, Q. Pan, J. Gao, C. Xie, and K. Peng, 2004, Phys. Rev. Lett. 93, 250503.
8. Takei, N., H. Yonezawa, T. Aoki, and A. Furusawa, 2005, Phys. Rev. Lett. 94, 220502.
9. Ralph, T. C., and P. K. Lam, 1998, Phys. Rev. Lett. 81, 5668.
10. Vaidman, L., 1994, Phys. Rev. A 49, 1473.
11. Wootters, W. K., and W. .H. Zurek, 1982, Nature 299, 802.
12. Buˇzek, V., and M. Hillery, 1996, Phys. Rev. A 54, 1844.
13. Cerf, N. J., A. Ipe, and X. Rottenberg, 2000, Phys. Rev. Lett. 85, 1754.
14. Lindblad G., 2000, J. Phys. A 33, 5059.
15. Grover, L. K., 1997, Phys. Rev. Lett. 79, 325.
16. Pati, A. K., S. L. Braunstein, and S. Lloyd, 2000, “Quantum searching with continuous variables”, arXiv:quant-ph/0002082v2.
17. Hoi-Kwan Lau, Raphael Pooser, George Siopsis, and Christian Weedbrook, 2017, Phys. Rev. Lett. 118, 080501
18. Логинов О.В., Цыганов А.В. Квантовый алгоритм Гровера (интернет-ресурс: http://old.exponenta.ru/educat/systemat/grover/index.asp)
19. P.W. Shor, AT&T Bell Labs., Murray Hill, NJ, USA, Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on
20. Daniel R. Simon, 1994, “On the power of quantum computation”, Microsoft corp. One Microsoft way. Redmond WA 9805206399
21. A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. 103, 150502 (2009).
22. Deutsch, D. (1985). «Quantum theory, the Church–Turing principle and the universal quantum computer». *Proceedings of the Royal Society* (400): 97–117.
23. «Введение в квантовое программирование на языке Quipper», Грин А. С., Лумсдайне П. Л., Росс Н. Дж., Зелингер П., Валирон Б. Университет

Далхаузи, Институт перспективных исследований, Университет Пенсильвании
24. IARPA Quantum Computer Science Program: Broad Agency Announcement IARPA-BAA-10-02 (April 2010), https://www.fbo.gov/notices/637e87ac1274d030ce2ab69339ccf93c.
25. https://www.haskell.org/platform/ - дистрибутив для языка Haskell.